Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1-34. (Canceled).

35. (Currently Amended) A method for authenticating a payment transaction over a network, comprising:

at a payment authentication service, storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

linking the PKI key pair to at least a first payment instrument of a buyer;

subsequent to the step of linking the PKI key pair to the first payment instrument and in response to receiving an authentication request from the buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, the seller separate from the payment authentication service, sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction;

subsequent to the step of linking the PKI key pair to the first payment instrument, receiving a selection of the first payment instrument from the buyer;

in response to receiving a challenge response from the buyer over the network, the challenge response including a summary of the payment transaction digitally signed by the buyer, ~~determining that the buyer has access to the private key and that the buyer is authorized to use the first payment instrument by using the public key to decrypt~~ decrypting the digitally signed summary of the payment transaction using the public key;

determining, from said decrypting, that the buyer has access to the private key and that the buyer is authorized to use the first payment instrument;

storing a digitally signed record of the payment transaction in a transaction archive; and

notifying the seller that the buyer is authorized to use the first payment instrument.

36. (Previously Presented) The method of claim 35, further comprising:

creating the PKI key pair; and

sending the private key to the buyer over the network.

37. (Previously Presented) The method of claim 35, wherein the record of the payment transaction is digitally signed using the private key.

38. (Previously Presented) The method of claim 35, wherein the record of the online transaction is digitally signed using a local private key.

39. (Previously Presented) The method of claim 35, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

40. (Previously Presented) The method of claim 35, further comprising:

retrieving a buyer profile from the database, the buyer profile being linked to the PKI key pair and including a plurality of payment instruments and a plurality of shipping addresses;

sending data from the buyer profile to the buyer over the network; and

receiving a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

41. (Previously Presented) The method of claim 35, further comprising:

processing the payment transaction via a payment gateway.

42. (Currently Amended) A computer readable medium storing instructions adapted to be executed by a processor, the instructions including a method for authenticating a payment transaction over a network, the method comprising:

at a payment authentication service, storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

storing a buyer profile that links the PKI key pair to at least a first payment instrument of

a buyer;

subsequent to the step of storing the buyer profile and in response to receiving an authentication request from the buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, the seller separate from the payment authentication service, sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction;

subsequent to the step of storing the buyer profile, receiving a selection of the first payment instrument from the buyer;

in response to receiving a challenge response from the buyer over the network, the challenge response including a summary of the payment transaction digitally signed by the buyer, ~~determining that the buyer has access to the private key and that the buyer is authorized to use the first payment instrument by using the public key to decrypt~~ decrypting the digitally signed summary of the payment transaction using the public key;

determining, from said decrypting, that the buyer has access to the private key and that the buyer is authorized to use the first payment instrument;

storing a digitally signed record of the payment transaction in a transaction archive; and

notifying the seller that the buyer is authorized to use the first payment instrument.

43. (Previously Presented) The computer readable medium of claim 42, wherein the method further comprises:

creating the PKI key pair; and

sending the private key to the buyer over the network.

44. (Previously Presented) The computer readable medium of claim 42, wherein the record of the payment transaction is digitally signed using the private key.

45. (Previously Presented) The computer readable medium of claim 42, wherein the record of the online transaction is digitally signed using a local private key.

46. (Previously Presented) The computer readable medium of claim 42, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

47. (Previously Presented) The computer readable medium of claim 42, wherein the method further comprises:

retrieving a buyer profile from the database, the buyer profile being linked to the PKI key pair and including a plurality of payment instruments and a plurality of shipping addresses;

sending data from the buyer profile to the buyer over the network; and

receiving a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

48. (Previously Presented) The computer readable medium of claim 42, wherein the method further comprises:

processing the payment transaction via a payment gateway.

49. (Currently Amended) A system for authenticating a payment transaction over a network, comprising:

a profile database;

a transaction archive; and

an authentication service web server coupled to the profile database, the transaction archive and the network, the authentication service web server adaptively configured to:

store a public key associated with a public key infrastructure (PKI) key pair in a profile database;

link the PKI key pair to at least a first payment instrument of a buyer;

subsequent to linking the PKI key pair to the first payment instrument, in response to receiving an authentication request from the buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, the seller separate

from the authentication service, send a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction;

subsequent to linking the PKI key pair to the first payment instrument, receive a selection of the first payment instrument from the buyer;

in response to receiving a challenge response from the buyer over the network, the challenge response including a summary of the payment transaction digitally signed by the buyer, ~~determine that the buyer has access to the private key and that the buyer is authorized to use the first payment instrument by using the public key to~~ decrypt the digitally signed summary of the payment transaction using the public key;

determine, from said decryption, that the buyer has access to the private key and that the buyer is authorized to use the first payment instrument;

store a digitally signed record of the payment transaction in a transaction archive; and

notify the seller that the buyer is authorized to use the first payment instrument.

50. (Previously Presented) The system of claim 49, wherein the authentication service web server is further adapted to:

create the PKI key pair; and

send the private key to the buyer over the network.

51. (Previously Presented) The system of claim 49, wherein the record of the payment transaction is digitally signed using the private key.

52. (Previously Presented) The system of claim 49, wherein the record of the online transaction is digitally signed using a local private key.

53. (Previously Presented) The system of claim 49, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

54. (Previously Presented) The system of claim 49, wherein the authentication service web server is further adapted to:

retrieve a buyer profile from the database, the buyer profile being linked to the PKI key pair and including a plurality of payment instruments and a plurality of shipping addresses;

send data from the buyer profile to the buyer over the network; and

receive a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

55. (Previously Presented) The system of claim 49, wherein the authentication service web server is further adapted to:

process the payment transaction via a payment gateway.

56. (Previously Presented) The method of claim 35, further comprising receiving confirmation that the buyer is authorized to use the first payment instrument prior to receiving the authorization request and prior to receiving the selection of the first payment instrument.

57. (Previously Presented) The computer readable medium of claim 42, wherein the method further comprises receiving confirmation that the buyer is authorized to use the first payment instrument prior to receiving the authorization request and prior to receiving the selection of the first payment instrument.

58. (Previously Presented) The system of claim 49, wherein the authentication service web server is further adapted to receive confirmation that the buyer is authorized to use the first payment instrument prior to receiving the authorization request and prior to receiving the selection of the first payment instrument.

59-64. (Canceled).